UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,043	12/17/2001	David E. McDysan	RIC01059	5663

25537 7590 03/24/2004

WORLDCOM, INC.
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW
WASHINGTON, DC 20036

EXAMINER	
HAMILTON, MONPLAISIR G	

ART UNIT	PAPER NUMBER
2135	12

DATE MAILED: 03/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,043	MCDYSAN, DAVID E.	
	Examiner	Art Unit	
	Monplaisir G Hamilton	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/2/04*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The communication filed on 1/2/04 added claim 21. Claims 1-21 remain for examination.

Priority

2. Applicant's claim for domestic priority under 35 U.S.C. 119(e) is acknowledged.

Response to Arguments

3. Applicant's arguments, see Paper No. 11, filed 1/2/04, with respect to the rejection of Claims 1-20 under 35 U.S.C. § 103(a) as obvious over Gleeson et al in view of Lewis et al, have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of US 20010016914 issued to Tabata.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-21 are rejected as being unpatentable over US 6079020 issued to Liu, herein referred to as Liu in view of US 2001/0016914 issued to Tabata, herein referred to as Tabata.

Referring to Claim 1:

Liu disclose a network system that resists denial of service attacks on an access link to a destination host belonging to a virtual private network (VPN), said network system comprising:

one or more egress boundary routers having connections to an access network including the access link (Fig. 1), wherein said one or more egress boundary routers transmit intra-VPN traffic from sources within the VPN and extra-VPN traffic from sources outside the VPN within separate access network logical connections for intra-VPN and extra-VPN traffic (col 7, lines 20-45; Fig 2); and

Liu does not explicitly disclose "a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented".

Tabata discloses a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (paragraph 0046, 0048; paragraph 0084; paragraph 0091), such that denial of service attacks on said access link originating from sources outside the VPN can be prevented (paragraph 0084).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Liu such that a denial of service attack is prevented. One of ordinary skill in the art would have been motivated to do this because it would prevent a bandwidth consumption attack (Tabata: paragraph 0084).

Referring to Claim 9:

Liu discloses a network system, comprising: an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (col 7, lines 20-45; Fig. 1-2);

Liu does not explicitly disclose "one or more egress boundary routers having connections to the access network, wherein said one or more egress boundary routers transmit intra-VPN traffic toward the destination host via the first logical connection and transmit extra-VPN traffic toward the destination host via the second logical connection; a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that

denial of service attacks on said access link originating from sources outside the VPN can be prevented"

Tabata disclose one or more egress boundary routers having connections to the access network, wherein said one or more egress boundary routers transmit intra-VPN traffic toward the destination host via the first logical connection and transmit extra-VPN traffic toward the destination host via the second logical connection (paragraph 0046; paragraph 0069; paragraph 0089); a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (Fig. 5paragraph 0046;), such that denial of service attacks on said access link originating from sources outside the VPN can be prevented (paragraph 0084; paragraph 0090-0093).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Liu such that a denial of service attack is prevented. One of ordinary skill in the art would have been motivated to do this because it would prevent a bandwidth consumption attack (Tabata: paragraph 0084).

Referring to Claim 16:

Liu discloses a method of protecting an access link to a destination host belonging to a virtual private network (VPN) against denial of service attacks, said method comprising: in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (col 7, lines 25-45);

Liu does not explicitly disclose "communicating, from a plurality of ingress boundary routers to one or more egress boundary routers, intra-VPN and extra-VPN traffic destined for said destination host, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic; transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented."

Tabata discloses communicating, from a plurality of ingress boundary routers to one or more egress boundary routers, intra-VPN and extra-VPN traffic destined for said destination host (Fig. 5; paragraph 0046), wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (paragraph 0064; paragraph 0069); transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection (paragraphs 0071-0073), such that denial of service attacks on said access link originating from sources outside the VPN can be prevented (paragraph 0084).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Liu such that a denial of service attack is prevented.

One of ordinary skill in the art would have been motivated to do this because it would prevent a bandwidth consumption attack (Tabata: paragraph 0084).

Referring to Claim 21:

Liu discloses a method for resisting denial of service attacks on an access link to a destination host included in a VPN, the method comprising the steps of: intra-VPN traffic flowing from sources included in the VPN (col 7, lines 25-45); extra-VPN traffic flowing from sources outside the VPN (col 7, lines 25-45);

Liu does not explicitly disclose "assigning a first priority level to traffic intra-VPN traffic flowing from sources included in the VPN; assigning a second priority level to traffic extra-VPN traffic flowing from sources outside the VPN; and granting, to traffic having the first priority level at the access link, precedence of access to the destination host over traffic having the second priority level."

Tabata discloses assigning a first priority level to traffic intra-VPN traffic flowing from sources included in the VPN; assigning a second priority level to traffic extra-VPN traffic flowing from sources outside the VPN; and granting, to traffic having the first priority level at the access link, precedence of access to the destination host over traffic having the second priority level (paragraph 0089).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Liu such that precedence information is used to partition the traffic. One of ordinary skill in the art would have been motivated to do this because it would prevent a bandwidth consumption attack (Tabata: paragraphs 0084-0087).

Referring to Claims 2, 10 and 17:

Liu in view of Tabata disclose the limitations of Claims 1, 9 and 16 above. Tabata further discloses a Differentiated Services network coupling at least one of the plurality of ingress boundary routers and at least one of the one or more egress boundary routers (paragraph 0063).

Referring to Claims 3 and 11:

Liu in view of Tabata disclose the limitations of Claims 1 and 9 above. Liu further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress boundary routers (col 5, line 60-col 6, line 10).

Referring to Claim 4:

Liu in view of Tabata disclose the limitations of Claim 1 above. Liu further discloses further comprising the access network (Fig. 1).

Referring to Claims 5 and 12:

Liu in view of Tabata disclose the limitations of Claims 4 and 9 above. Liu further discloses a customer premises equipment (CPE) edge router to the access link (Fig. 1; col 6, lines 1-25).

Referring to Claims 6, 13 and 18:

Liu in view of Tabata disclose the limitations of Claims 5, 12 and 16 above. Tabata further discloses said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (paragraph 0069).

Referring to Claims 7, 14 and 19:

Liu in view of Tabata disclose the limitations of Claims 1, 9 and 16 above. Tabata further discloses at least one of said plurality of ingress boundary routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic (paragraph 0108).

Referring to Claims 8, 15 and 20:

Liu in view of Tabata disclose the limitations of Claims 1, 9 and 16 above. Tabata further discloses said one or more egress boundary routers provide a plurality of different qualities of services to said intra-VPN traffic (paragraph 056-0058; paragraph 0101).

Prior Art

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 20020075901 issued to Perlmutter, Bruce et al. Perlmutter discloses allocation of bandwidth to a link, which is remotely displaced from a server, is described. The link need not directly connected to the server. The server includes a process to assign a portion of the bandwidth to at least one application group; and count packets belonging to the application

group that pass through the server. The server can be a VPN server that authenticates packets. Each application group includes packets that share a pre-defined configuration. Accordingly, the server combines bandwidth management and packet authentication with little overhead.

US 6618761 issued to Munger, Edmund Colby et al. Munger discloses methods and systems allowing a plurality of computer nodes to communicate using weighted transmission paths are provided. A load balancer distributes packets across weighted transmission paths according to transmission path quality, which is monitored and updated from time to time. As transmission quality on a specific transmission path decreases, the weight assigned to that transmission path is reduced. Similarly, weights may be increased if transmission quality improves. The weights assigned to various transmission paths may correspond to a relative number of packets to be transmitted on each respective transmission path. The transmission path for each packet can be selected based on the weights of the various transmission paths. Using weights based on transmission quality, transmission paths with higher transmission quality are used more often than transmission paths with lower transmission quality, resulting in more efficient communications.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monplaisir G Hamilton whose telephone number is (703) 305-5116. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Monplaisir Hamilton